4-2019

# Feasibility and Security Analysis of Wideband Ultrasonic Radio for Smart Home Applications

Qi Xia
*University of Nebraska-Lincoln*, qxia@huskers.unl.edu

# FEASIBILITY AND SECURITY ANALYSIS OF WIDEBAND ULTRASONIC RADIO FOR SMART HOME APPLICATIONS

by

Qi Xia

A THESIS

Presented to the Faculty of

The Graduate College at the University of Nebraska

In Partial Fulfilment of Requirements

For the Degree of Master of Science

Major: Computer Science

Under the Supervision of Professor Qiben Yan

Lincoln, Nebraska

April, 2019

# FEASIBILITY AND SECURITY ANALYSIS OF WIDEBAND ULTRASONIC RADIO FOR SMART HOME APPLICATIONS

Qi Xia, M.S.

University of Nebraska, 2019

Adviser: Qiben Yan

Smart home Internet-of-Things (IoT) accompanied by smart home apps has witnessed tremendous growth in the past few years. Yet, the security and privacy of the smart home IoT devices and apps have raised serious concerns, as they are getting increasingly complicated each day, expected to store and exchange extremely sensitive personal data, always on and connected, and commonly exposed to any users in a sensitive environment. Nowadays wireless smart home IoT devices rely on electromagnetic wave-based radio-frequency (RF) technology to establish fast and reliable quality network connections. However, RF has its limitations that can negatively affect the smart home user experience and even cause serious security issue, such as crowded spectrum resources and RF waves leakage. To overcome those limitations, people have to use technology with sophisticated time and frequency division management and rely on the assumptions that the attackers have limited computational power. In this thesis we propose URadio, a wideband ultrasonic communication system, using electrostatic ultrasonic transducers. We design and develop two different types of transducer membranes using two types of extremely thin materials, Aluminized Mylar Film (AMF) and reduced Graphene Oxide (rGO), for assembling transducers, which achieve at least 45 times more bandwidth than commercial transducers. Equipped with the new wideband transducers, an OFDM communication system is designed to better utilize the available 600 kHz wide bandwidth. Our experiments show that

URadio can achieve an unprecedentedly 4.8 Mbps data rate with a communication range of 17 cm. The attainable communication range is increased to 31 cm and 35 cm with data rates of 1.2 Mbps and 0.6 Mbps using QPSK and BPSK, respectively. Although the current wideband system only supports short-range communication, it is expected to extend the transmission range with better acoustic engineering. Also, by conducting experiments to measure the ultrasonic adversaries' eavesdropping and jamming performance, we prove that our system is physically secure even when exchanging plaintext data.

# Table of Contents

## List of Figures

# List of Tables

# Chapter 1

# Introduction

## 1.1 Motivation

In the past few years, smart home Internet-of-Things (IoT) devices have experienced tremendous growth. Intelligence and sophistication of home automation systems, remote control system and human-machine interaction system, which provide all types of appliance information and data exchanging infrastructure and services, are increasing rapidly year by year.

Radio Frequency (RF) based communication protocols, such as WiFi, Bluetooth, Zigbee, and Z-wave, have been used to connect IoT devices. However, since the signal travels in the form of electromagnetic wave, which has the properties of wide spreading, omnidirectional and penetrating, IoT devices are inherently susceptible to the common attacks towards wireless networks, including radio jamming [1], eavesdropping [2], and signal manipulation attacks [3].

Airborne ultrasonic communication has recently aroused many researchers' interests due to its advantages over traditional RF communication, which suffers from strict frequency spectrum regulation, severe interference with an increasing number of devices crowd in a narrow bandwidth and aggregating security concerns in an adverse environment. Ultrasonic data transmission, on the other hand, due to its Line-of-sight

(LoS) transmission property, can be implemented using any acoustic frequency bands in an interference-free manner. Also, there is currently no regulation on ultrasound spectrum usage. Moreover, compared with RF signals, ultrasonic signals attenuate greatly in the air and has much shorter wavelength compared with its electromagnetic wave counterpart at the same frequency, which makes it difficult to intercept, as highly-directional ultrasonic signals can only transmit effectively over the *line of sight (LoS)* links, and could not penetrate through solid walls [4]. These unique features of ultrasonic communication greatly reduce its exposure risks to the eavesdroppers and jammers. However, airborne ultrasonic communication suffers from limited bandwidth due to the severe propagation loss of ultrasound at MegaHertz frequency and the limited bandwidth of existing ultrasonic transducers.

Recent studies have investigated practical ultrasonic data transmission with real system implementations. In [5], a wearable ultrasonic communication system, U-Wear, is implemented to achieve a data rate of 2.76 Kbps using Gaussian Minimum Shift Keying (GMSK) modulation. In [6], an ultrasonic communication system is developed that exploits the nonlinear behavior of the microphone's membrane to transform an ultrasonic signal into an audible signal, which achieves a data rate of 4 Kbps. Chirp and Multiple Frequency-Shift Keying (MFSK) modulation have also been used to transmit inaudible signals at 16 bps and 800 bps, respectively [7, 8]. These low data rate transmission systems meet the needs for some IoT applications with intermittent data exchanges, e.g., text messaging, command-and-control, cross-device tracking, and targeted advertising [9].

However, in today's world, online picture browsing, large file sharing, or even video streaming require a large quantity of modern smart home applications to achieve a data rate exceeding 1 Mbps. Yet, designing a high-speed ultrasonic communication system is practically challenging due to the limitation of an ultrasonic transducer

bandwidth. To the best of our knowledge, there exist two airborne ultrasonic communication systems that achieve a data rate of over 100 Kbps. Li et al. propose a Quadrature Phase-Shift Keying (QPSK) modulated system that achieves a data rate of 200 Kbps over 1.2 m [10]. Jiang et al. further propose an OFDM-based ultrasonic communication [11] using a pair of lab-made transducers to achieve a data rate of 800 Kbps with 16-QAM over a range of 0.7 m.

## 1.2 Our Solution

In an acoustic transducer such as a microphone, air pressure (sound wave) induce motion of a suspended diaphragm, which is in turn converted to an electrical signal. *The key to achieving wideband ultrasonic communication is to have a lightweight but mechanically strong diaphragm for sound generation/detection.* Thinner and lighter diaphragms allow for more faithful tracking of sound vibration at high frequencies and stronger material make the diaphragm to stay intact during vibration. Graphene, being only one-atom-thick (0.33 nm) and mechanically strong, constructs the ultra-lightweight diaphragms. However, Graphene diaphragms have been shown to be extremely brittle and subject to be fractured [12]. On the other hand, reduced Graphene Oxide (rGO) has sufficient mechanical strength while preserving the thinness [13].

In this thesis, we present URadio, the *fastest* ultrasonic communication system equipped with three different types of transducers, including a commercial-off-the-shelf (COTS) transducer and two pairs of lab-made transducers, one of which uses *Aluminized Mylar Film (AMF)* with a thinness of 2 $\mu$m and the other uses *reduced Graphene Oxide (rGO)* membrane measured as 0.4 $\mu$m. We design an electrostatic ultrasonic transducer structure integrated with the membranes to achieve the highest reception sensitivity. URadio implements OFDM modulation to better utilize the

wide bandwidth that is made available by the newly designed transducers. We thoroughly test the URadio system and show the high speed, efficiency, and security of the proposed system.

## 1.3 Contributions

To sum up, this thesis makes the following contributions:

- We developed two types of acoustic membranes for transducers to achieve wideband ultrasonic communication. We design an OFDM based communication system, URadio, to utilize the wide bandwidth for high-speed ultrasonic communication.

- When equipped with COTS transducers, our system can achieve an error-free transmission of 10.3 m at a data rate of 20 Kbps using BPSK modulation scheme. When equipped with lab-made transducers, the communication data rate can reach up to 4.8 Mbps using 64-QAM at an attainable range of 17 cm in an error-free manner.

- Our ultrasonic communication system can operate in an interference-free manner coexisted with RF systems in overcrowded RF environments or ultrasonic environment. We evaluate image transfer capability of URadio, proving that URadio can satisfy the need for high-speed data exchange among smart home devices. We also show the system's resistance against jamming and eavesdropping attacks. By performing two sets of indoor experiments, we demonstrate that URadio can achieve a secure and high data rate transmission for smart home applications.

# Chapter 2

# Related work

## 2.1 Ultrasonic Data Transmission

In this chapter, additional relevant previous work that has not been mentioned before are reviewed. Using ultrasound as a carrier to achieve data transmission has long been investigated. Jiang et al. [14] achieved a full-duplex point-to-point ultrasonic transmission by using two pairs of transducers, a function generator, and an oscilloscope. U-Wear [5] goes beyond a simple point-to-point transmission scheme by interconnecting multiple wearable devices using ultrasound.

Since ultrasound signals are inaudible, they can be used as hidden signals for smart home devices, for both benign and malicious purposes. The nonlinear behavior of MEMS microphones has been utilized to achieve data transmission [6]. Zhou et al. enable real-time unobtrusive speaker-microphone data communication using ultrasonic signal [15], without affecting the primary audio-hearing experience of human users.

## 2.2 Ultrasonic Inaudible Attacks

Also, the ultrasonic signal can be used maliciously to launch inaudible attacks, which pose a threat to smart home security. In [16, 17], adversaries exploit the microphones' non-linearity and send inaudible ultrasound to force the microphone to record malicious ultrasonic signals as normal voice commands, thereby hijacking the voice recognition system.

Small mechanic components at the scale of ultrasound wavelength in devices, such as sensors, hard disk read-and-write head, are also susceptible to an airborne ultrasonic attack that exploits their mechanical resonant frequency. Bolton et al. launch an ultrasonic attack on a mechanic hard disk drive, causing physical causality and even OS failures [18]. Security researchers inject well-designed ultrasonic signals with specific frequencies to sensors (i.e., gyroscope, accelerometer, etc), achieving a denial-of-service attack or even arbitrary manipulation of sensor outputs [19–21]. While these ultrasonic attacks towards smart home devices are devastating, we propose URadio to use ultrasound to secure smart home communication.

# Chapter 3

# Airborne Ultrasonic Communication

## 3.1 Ultrasonic Communication Background

Ultrasonic signal constitutes of longitudinal mechanical waves propagating in elastic media (e.g., air) with a frequency above 20 kHz. Similar to RF signals, two main factors contribute to ultrasound's attenuation over the air, i.e., *path loss* and *absorption*. The former includes free-space loss, refraction, diffraction, reflection, and aperture-medium coupling [22], while the latter factor denotes the absorption of ultrasound waves in the air that is largely depending on the temperature, pressure and moisture [23].

The propagation speed of acoustic waves in air is approximate 340 m/s at a temperature of 20°C under an atmospheric pressure of 101.325 KPa, compared to $3 \times 10^8$ m/s for RF waves. The low transmission speed brings a greater propagation delay for data transmission across a long distance, which makes it well suited for security-sensitive short-distance indoor applications.

**Air-coupled ultrasonic transducers.** Ultrasonic transducers serve as converters to transform sound wave into electrical current or vice versa. Ultrasonic transducers nowadays can be categorized into two main classes based on their physical mechanisms, i.e. *piezoelectric* and *electrostatic transducers*. Piezoelectric transducers con-

vert voltage variation into mechanical vibration through a piezoelectric element, which can work under a low AC voltage level. However, a piezoelectric transducer usually has a very narrow resonant bandwidth typically at 1 kHz. Electrostatic transducers convert voltage variation into mechanical vibration using a membrane excited by an electrostatic force. Electrostatic transducers require a high DC voltage between the membrane and the electrode to drive the membrane's vibration, but they introduce a wider communication bandwidth, thereby enabling a higher data rate communication.

## 3.2 Threat Model in Smart Home Communications

Smart home IoT devices have been developed for in-home security monitoring and the convenience of living. Smart home technologies rely on instant and reliable communication between IoT devices. However, RF-based IoT devices are susceptible to a wide range of attacks due to the physical properties of the RF signals. These attacks can be categorized into passive attacks and active attacks [24]. The passive attackers can utilize the wide-spreading property of RF signals to passively collect the transferring information without being detected, i.e., launching eavesdropping attacks. An active attacker may attempt to alter system resources or disrupt its normal operation by transmitting RF signals to the receivers. The active attack includes masquerading, replay, message modification, denial of service (DoS), etc. Although countermeasures exist at upper layers to ensure confidentiality, integrity, and availability, the physical layer security threats are difficult to counteract. Particularly, the eavesdropping attacks impose serious threats to a smart home environment in the presence of insider adversaries that have access to encryption keys.

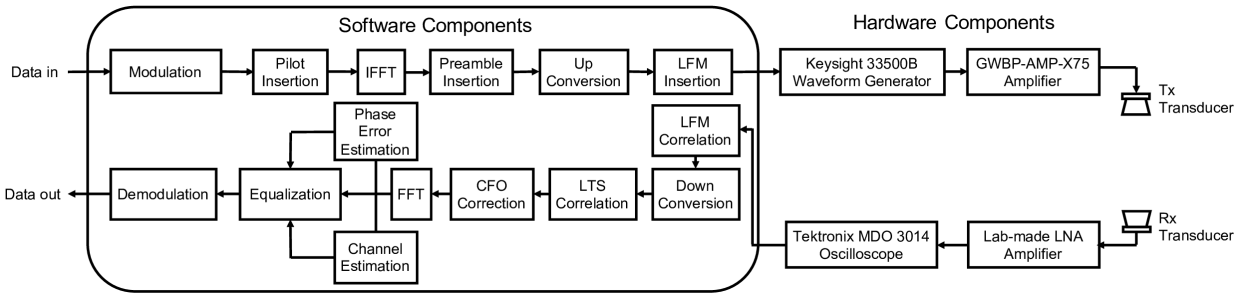



Figure 3.1: URadio system architecture.

## 3.3 Problem Formulation

By substituting RF based smart home devices with its ultrasound-based counterparts, the device would be much less vulnerable to the above-mentioned security threats. Compared with RF signals, the ultrasonic signal can barely penetrate through solid materials such as doors and walls. Ultrasonic signals attenuate faster across the air and can only efficiently travel through LoS links. Since the jamming and eavesdropping attacks require the signals to be dispersing, ultrasonic communication system becomes physically more secure. But the same property also limits the available bandwidth of ultrasonic communication. There seems to be an intrinsic conflict between achievable bandwidth and security. To make ultrasonic communication a reality, we need to develop a secure ultrasonic system that satisfies the bandwidth requirement. In this thesis, we develop a system, URadio, to effectively resolve the conflict between wideband communication and security. Not only is URadio a wideband communication system, it simultaneously achieves jamming-resilient communication, and is immune to eavesdropping attackers who are off the LoS path.

# Chapter 4

# URadio System Design

URadio consists of a set of software components and hardware components. The hardware components include a transducer and amplify circuit design, and the software components implement an OFDM-based ultrasonic communication system. Fig. 3.1 presents the complete URadio system architecture.

## 4.1 Transducer Design

URadio has been equipped with three different types of transducers, including a COTS transducer (SensComp 600 series) and two pairs of lab-made transducers, to achieve wideband ultrasonic data transmission. The ultrasonic transducer, as a frontend, is of utmost importance in ultrasonic communication, which serves as an interface to the physical environment.

Most of the COTS ultrasonic transducers suffer from a narrow bandwidth. Compared with COTS piezoelectric sensors, capacitive ultrasonic transducers have relatively broader bandwidth. We choose a capacitive ultrasonic transducer, SensComp 600 series instrument grade ultrasonic sensor [25], to be integrated into URadio, which is shown in Fig. 4.1. These sensors are made of a gold foil coated polymer membrane and an Aluminum backplate with a diameter of 38.4 mm. The SensComp transduc-

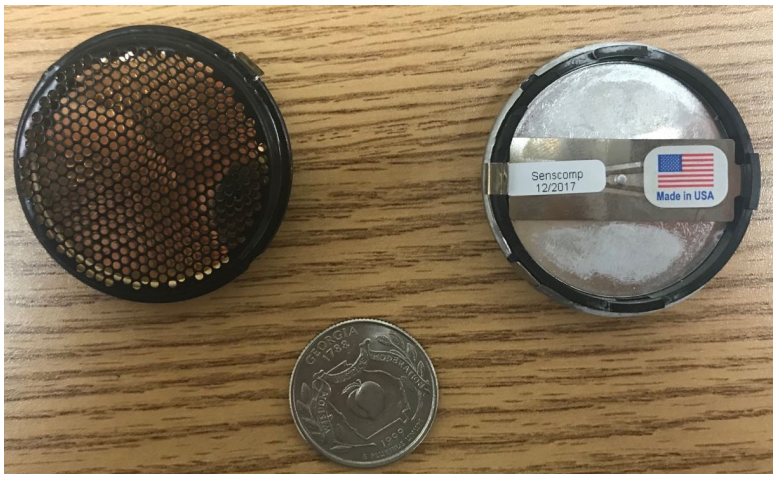



Figure 4.1: SensComp series 600 ultrasonic transducer.

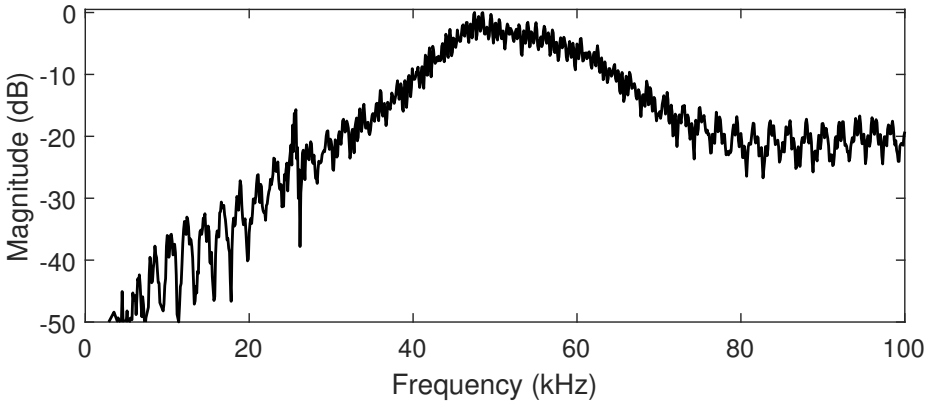



Figure 4.2: Frequency response of a pair of SensComp transducers placed one meter from each other.

ers operate at a relatively low-frequency range between 45 kHz and 65 kHz. The frequency response of SensComp is measured and presented in Fig. 4.2, which shows the peak frequency response at around 50 KHz.

For high data rate transmission, the bandwidth should be extended. However, the response of a traditional transducer, which measures the voltage variation of the vibrating membrane, will reduce as the frequency rises. Therefore, we need to develop wideband transducers using thinner materials. Formally, the movement of a diaphragm could be modeled as a second-order spring-damping-mass system, where the mass comes from the diaphragm, the damping force comes from the air, and the

spring represents the restoring force that brings diaphragm to the balanced position. Therefore, the formula that describes the movement of the diaphragm can be written as:

$$F = m\frac{d^2x}{dt^2} + \zeta\frac{dx}{dt} + kx, \tag{4.1}$$

where $x$ is the displacement of the diaphragm, $t$ is the time, $m$ is the mass of diaphragm, $\zeta$ is the damping coefficient, $k$ is the spring constant, and $F$ is the driving force applied on the diaphragm. When driven by a sinuous signal at frequency $f$, the vibration amplitude can be written as:

$$|\frac{dx}{dt}| = \frac{|F|}{|\zeta + i(2\pi fm - (2\pi f)^{-1}k)|}. \tag{4.2}$$

Here, the vibration amplitude is represented in the form of velocity rather than displacement, because the *sound pressure level (SPL)* is directly determined by the velocity amplitude of air:

$$SPL = c\rho|\frac{dx}{dt}|, \tag{4.3}$$

where $c$ is the sound velocity and $\rho$ is the mass density of air. From the above equations, we note that larger mass $m$ results in poorer high frequency response (i.e., $f$ in Eq. (4.2)). As a result, the mass density of the diaphragm sets an upper limit on the frequency response of a transducer. It is thus clear that, in order to extend the bandwidth, thinner and lighter diaphragms should be employed for more faithful tracking of sound vibration at higher frequencies.

Fig. 4.3 illustrates the structure of the transducers, which we design and produce using a 3D printer (the device is displayed in Fig. 4.4(a)). Briefly, the transducer is built with an AMF membrane (2 $\mu$m thick, 7 mm in diameter) or an rGO membrane (0.4 $\mu$m thick) suspended midway between two perforated electrodes, which

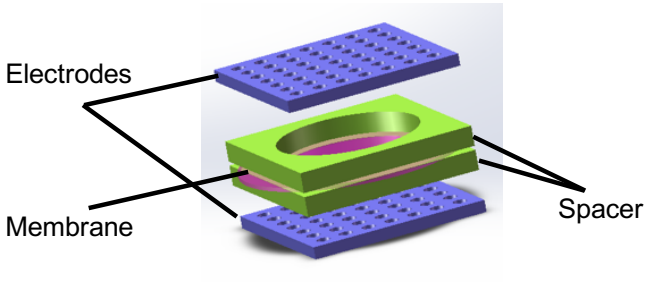



Figure 4.3: The 3D structure of a transducer with a membrane separated by two perforated electrodes with two spacers.

are constructed by a stainless steel is woven mesh sheet. Spacers, which are made of polyethylene terephthalate (PET) sheet (100 um thick), sandwiches the membrane, preventing it from touching the electrodes. For the transmitter (or speaker), the electrical signal and the inverse of the signal are sent to the two electrodes separately. According to Coulomb's law, the voltage changes on the electrode result in mechanical movements of the membrane, which further result in mechanic movements of air according to Eq. (4.3). The air movements are then transformed into acoustic waves, penetrating the electrodes and traveling over the air. The receiver (or microphone) works in reverse order: the airborne acoustic wave can penetrate through the electrodes to displace the membrane, thereby changing the capacitance between the membrane and electrodes, and in turn causing charge redistribution and electrical currents, which are the signals we aim to capture.

## 4.2 Design and Assembly of Membranes

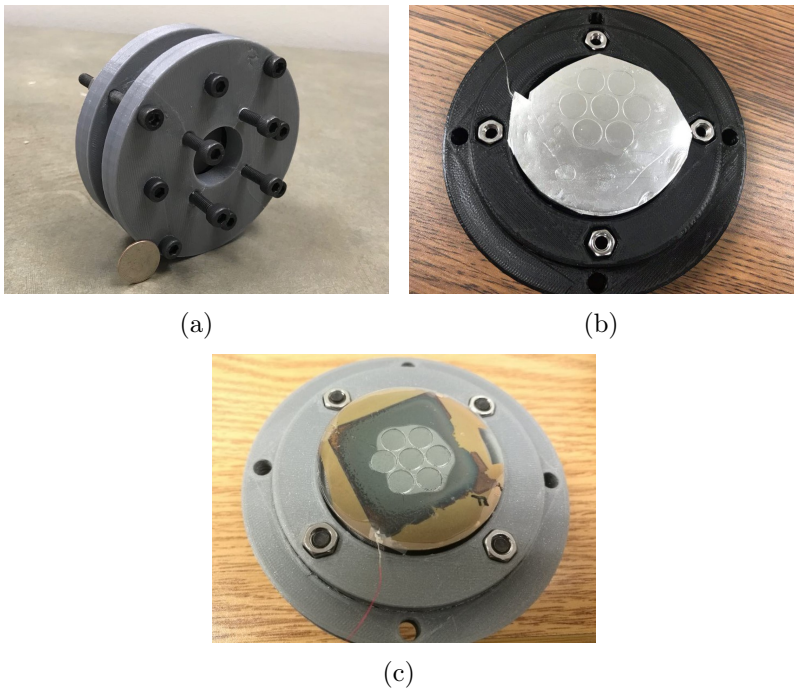
**Aluminized Mylar Film (AMF) membrane development and assembly.** We first choose Aluminized Mylar material to produce a membrane. Compared with reduced Graphene Oxide (rGO) membrane, AMF membrane is less sensitive to acoustic wave but are easier to fabricate, because aluminized sheet can be easily purchased as COTS and needs no further processing. We cut seven holes on two PET sheets, and

glue the AMF membrane in between them as shown in Fig. 4.4(b). After that, the membrane is sandwiched between two electrodes and assembled into the 3D-printed transducer structure as shown in Fig. 4.4(a).

**reduced Graphene Oxide (rGO) membrane fabrication.** The rGO membranes are relatively difficult to fabricate compared with its AMF counterpart. The whole fabrication process is based on drop casting method [26]. The Graphene Oxide (GO) water dispersion for drop casting is first prepared by dissolving and sonicating 0.5 ml commercial ultra-high concentration graphene oxide aqueous solution (6.2g/L) in 2 ml high purity water. The GO water dispersion is then dropped cast onto a piece of $SiO_2$ wafer putting on the hotplate. After 105°C baking, a GO thin film is formed on the $SiO_2$ substrate. The $SiO_2$ substrate with solid GO membrane is then immersed into the hydroiodic acid for 10 min of chemical reduction. After that, the $SiO_2$ is withdrawn from the acid and put into high purity water container to rinse and to maintain the hydrophobic property of rGO surface. Finally, the rGO membrane will naturally be separated from $SiO_2$ and floats on the water surface. A Kapton tape can be used to pick up the membrane to suspend for Ultimate Tensile Strength (UTS) measurement and deployment. A small flake was cut off to measure thickness by Atomic Force Microscopy (AFM). The measurement indicates that the diluted rGO membrane is about 400 nm (or 0.4 $\mu$m) with a minimum UTS of 191 MPa. Fig. 4.4(c) shows a well-fabricated rGO membrane. After the membrane is made, it can be assembled into the 3D-printed transducer structure.

## 4.3 Amplifier Circuit Design

The signals directly captured from the membrane vibration are extremely weak signals, which require amplification for further processing. URadio incorporates two



(a) (b)

(c)

Figure 4.4: The assembled transducers: (a) 3D-printed transducer; (b) an assembled transducer with AMF membrane; (c) an assembled transducer with rGO membrane.

types of amplifiers including a power amplifier (PA) at the transmitter and a low noise amplifier (LNA) at the receiver, since the received signal at the receiver is particularly susceptible to noise.

At the transmitter, we choose a commercial power amplifier with an operational frequency ranging from 50 kHz to 1.2 MHz and a voltage gain of 40 dB and a maximum voltage of 27 V. The LNA at the receiver requires an extremely low noise figure ($<$ 13 dB) to constrain noises' impacts, with a broad bandwidth (at least 100 kHz - 1 MHz) and a high gain (at least 35 dB), especially when the system performs high-speed data transmission. The COTS amplifiers are usually either too narrow in bandwidth or too high in noise figure. Only a few specially designed LNA can meet the needs. Here, we design our own LNA system. At the receiver side, two chips, OPA637BP and OPA1611 are employed to build a 2-stage amplifier circuit with a high gain up to 30 dB, a broad bandwidth from DC to 1 MHz. Fig. 4.5 shows the schematic

diagram of the designed circuit. Since the circuit copes with extremely weak electric current (down to 10 $\mu$A), it has to be designed in a way that allows the electronic components in the circuit to be isolated. Therefore, the electronic components have to be soldered on a copper board with pins off the ground. Self-excitation easily occurs in this 2-stage amplifier circuits due to the high gain (i.e., 30 dB or equivalent to $1,000\times$ gain). To suppress self-excitation, a customizable small capacitor (i.e., C2 in Fig. 4.5) is used to connect the input and the output of the first-stage amplifier, shifting the self-exciting frequency of this circuit to a much higher frequency (>10 MHz), thereby effectively suppressing it. As is shown in Fig. 4.6, the frequency response of this 2-stage amplifier circuit has a broad operational *3 dB bandwidth* from DC to 1 MHz. After assembling AMF transducers, we measure the frequency response of transmitter and receiver transducers integrated with the amplifier circuit, the result of which is shown in Fig. 4.7. Compared with Fig. 4.2, the URadio system integrated with AMF transducers presents a wide 3 dB bandwidth from 60 kHz to above 1 MHz that can be used for ultrasonic communication, which indicates at least $45\times$ more bandwidth than SensComp transducers. The frequency response drops between DC to 60 kHz, which is caused by the transmitter side power amplifier who has a cutoff operational frequency around 50 to 60 kHz.

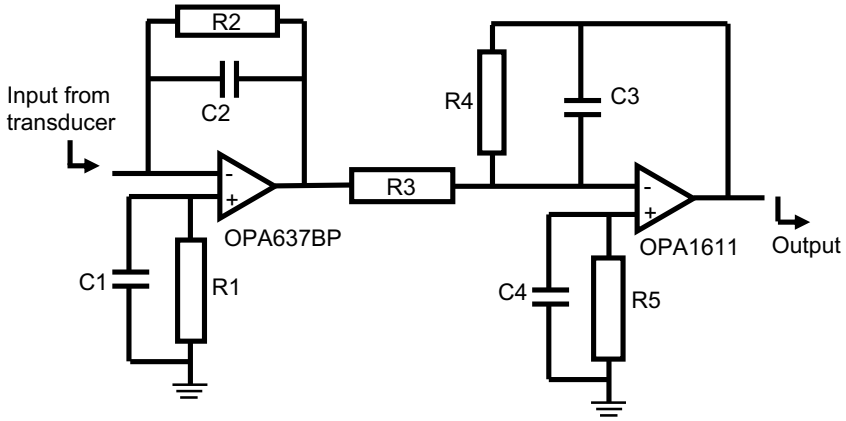



Figure 4.5: The schematic diagram of LNA circuit (C1 – C4 are capacitors, and R1 – R5 are resistors).

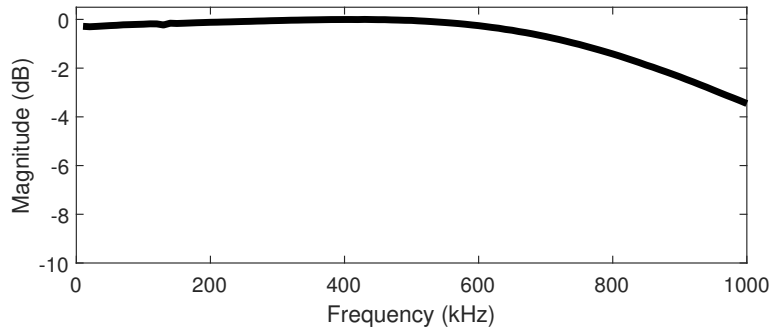



Figure 4.6: The frequency response of LNA circuit.

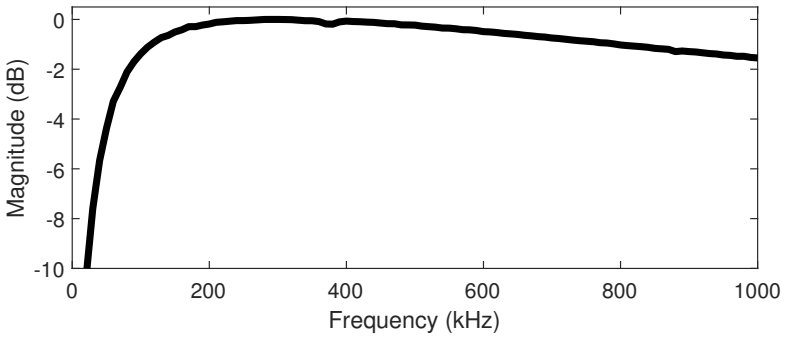



Figure 4.7: Frequency response of AMF transducers (integrated with amplifier circuits) over a distance of 20 cm.

## 4.4 Wideband Ultrasonic OFDM Communication System Design

In URadio, due to the available wide bandwidth, OFDM modulation is used to maximize the spectrum utilization. We follow the WiFi protocol by embedding 52 subcarriers into one OFDM symbol. We utilize linear frequency modulation (LFM) to achieve frame synchronization. Similar to WiFi, a long training sequence (LTS) is used to achieve fine-grained time synchronization. Carrier Phase Offset (CFO) correlation is used to correct the distortion of the baseband signal. Then, phase error estimation and channel estimation are performed to estimate the channel response and mitigate the channel distortion, thus making the system adaptive to different

types of channels. The complete OFDM modulation and demodulation process are shown in Fig. 3.1, while the structure of our OFDM-based frame is shown in Fig. 4.8.

### 4.4.1 Synchronization

Synchronization in URadio is achieved in two steps. First, the receiver identifies any incoming packet via coarse synchronization, which relies on an LFM signal located at the beginning of each packet and served as a preamble. Once a packet is detected, a fine synchronization will be processed by the receiver to determine the exact starting time of packet payload. The fine synchronization is achieved by correlating the down-converted signal with a local copy of preamble, i.e., LTS. The correlation peaks at the received symbol's starting position.

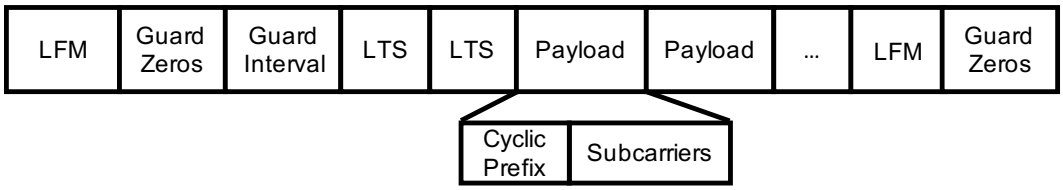



Figure 4.8: The structure of an OFDM-based frame.

The LFM preamble is a sinusoidal waveform whose frequency varies linearly from an initial frequency $f_0$ to an end frequency $f_1$ within a certain time period $T$. LFM signal is also called a chirp signal, which is widely used in radars due to its superior autocorrelation and robustness against additive stochastic noise [27]. The LFM signal can be described as the following formula:

$$S(t) = A \cdot cos(2\pi t(f_0 + k/2 * t) + \phi), \tag{4.4}$$

where $f_0$ is the starting frequency, $k$ is the rate of frequency change, $A$ is the amplitude, and $\phi$ is the phase. The correlation peaks of the received signal with a local copy of LFM indicates the start of the arriving data sequence.

After the frame synchronization and downconversion, we use a cross-correlator to search for the 64-sample LTS in the preamble to achieve a fine synchronization. An LTS preamble consists of a sequence of {-1, 1}. Fig. 4.8 shows two successive LTS used in an OFDM frame. The two LTS preambles are used to precisely locate the start of a packet payload, marking the boundary of each OFDM frame fed into the FFT module.

### 4.4.2 Channel Estimation

Ultrasonic communications over the air are greatly affected by frequency selectivity and multipath fading of an ultrasonic channel. In URadio, LTS is used to estimate the channel impulse response (CIR) and compensate for the channel distortion, in order to turn the frequency-selective channel into a flat channel. During the demodulation, the LTS preambles at the beginning of each package that is known by the receiver are used to correct the phase and amplitude of the received OFDM signals. Thus, the channel estimation $H_{est}$ can be expressed as:

$$H_{est} = LTS * (LTS'_1 + LTS'_2)/2,$$

where $LTS'_1$ and $LTS'_2$ are the FFT results of first and second LTS of the received signal, and $LTS$ is a known LTS copy.

### 4.4.3 Bandwidth Selection

The operational bandwidth of this system is restricted by two factors: the transducers' resonant frequency and the orthogonality of the carrier signals. As a rule of thumb, the operational bandwidth should be centered around the transducers' resonant frequency. In URadio, we use correlation demodulator to achieve downcon-

version at the receiver side. When the carrier frequency $f_c$ is not far greater than the bandwidth, strict orthogonal condition is required for the correlation demodulator to operate successfully. The orthogonal condition can be described as follows:

$$\int_0^{T_s} cos(2\pi f_c t) sin(2\pi f_c t) dt = 0, \tag{4.5}$$

where $T_s$ is the duration of one symbol, and $T_s = 1/BW$, where $BW$ is the bandwidth. Via simple derivation from Eq. (4.5), we can get: $sin^2(2\pi f_c T_s) = sin^2(2\pi f_c/BW) = 0$. Therefore, to maintain such an orthogonality, carrier frequency has to be an integer multiple of a half bandwidth:

$$\frac{f_c}{BW} = \frac{n}{2}, \tag{4.6}$$

where $n \in Z$ and $n \geq 1$. Let $f_h$ and $f_l$ donate the high and low cutoff frequency of a symbol, then $f_c = (f_h + f_l)/2$, $BW = f_h - f_l$. Therefore, Eq. (4.6) can be further expressed as:

$$f_h = \frac{n+1}{n-1} f_l. \tag{4.7}$$

Eq. (4.7) implies that the bandwidth (or the difference between $f_h$ and $f_l$) is inversely proportional to $n$, and $n \geq 1$. As $f_l \neq 0$ and $f_h \neq \infty$, $n \geq 2$. Thus, we choose $n = 2$, $f_h = 900$ kHz, $f_l = 300$ kHz with a bandwidth of 600 kHz for our lab-made AMF and rGO transducers.

# Chapter 5

# Performance Evaluation

We implement URadio system including both hardware and software components. In this chapter, we conduct comprehensive experiments to evaluate the performance of URadio system. We perform the experiments in a lab environment, and measure URadio's communication and security performance.

## 5.1 Experimental Setup

Fig. 5.1 presents the experimental arrangement for this ultrasonic communication system. The data is processed and modulated by MATLAB programs that run on a laptop before sending to a Keysight 33500B waveform generator using a general purpose interface bus (GPIB). The signals from the waveform generator are amplified by two GWBP-AMP-X75 Power Amplifiers. The two amplifiers are powered by DC power supplies with a voltage of 24 V and cooled down using two fans. The signals are then transmitted by our ultrasonic transducer. Travelling through the air, the air-coupled ultrasonic signals are then captured by another ultrasonic transducer that is connected to an LNA hosted in a Faraday box. The Faraday box is used to shield electromagnetic interference from RF signals. The amplified signals are then digitized by a Tektronix oscilloscope and sent back to the laptop for post-processing via an

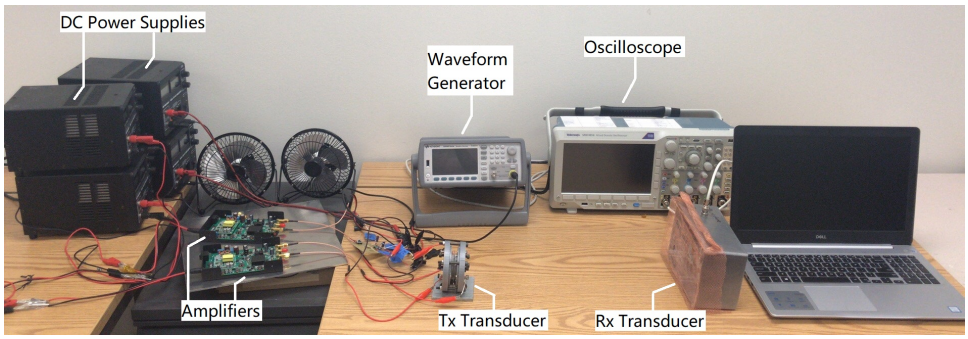



Figure 5.1: An illustration of the benchtop experimental setup for URadio communication.

Ethernet cable.

## 5.2 Experimental Results of Communication Capability

We conduct the experiments in an indoor lab environment with no detectable ultrasonic background noise. The transmitter and receiver exchange ultrasonic signals over an LoS link. Four different types of baseband modulation schemes, i.e., BPSK, QPSK, 16-QAM, and 64-QAM, are used to modulate the OFDM subcarrier signals that range from 45 to 65 kHz in the URadio system with SensComp transducers, or cover from 300 to 900 kHz in the URadio system with the lab-made AMF and rGO transducers.

Our first experiment evaluates and compares the performance metrics such as bandwidth, data rate, transmission range, SNR, bit error rate (BER) of all the four modulation schemes using SensComp, AMF, and rGO ultrasonic transducers. The BER performance is measured by fixing the communication range (1 m for SensComp, 15 cm for lab-made transducers) and tuning the transmission power. Each 140 byte packet signal is transmitted 10 times. The maximum transmission range using our current instruments with non-detectable BER is listed in Table 5.1. As can be seen from Table 5.1, URadio achieves a high date rate of 1.2 Mbps, 2.4 Mbps, and 4.8

Table 5.1: URadio communication performance.

| Transducers | Mod Type | $f_c$ (kHz) | BW (kHz) | Data Rate (Kbps) | Range (cm) | SNR (dB) | BER |
|---|---|---|---|---|---|---|---|
| SensComp | BPSK | 50 | 20 | 20 | 1,030 | 9 | $<$ 1e-4 |
| | QPSK | | | 40 | 680 | 10.2 | |
| | 16QAM | | | 80 | 440 | 15.5 | |
| | 64QAM | | | 160 | 350 | 17.7 | |
| AMF | BPSK | 600 | 600 | 600 | 27 | 8.1 | $<$ 1e-4 |
| | QPSK | | | 1,200 | 25 | 9.8 | |
| | 16QAM | | | 2,400 | 20 | 15.9 | |
| | 64QAM | | | 4,800 | 15 | 18 | |
| rGO | BPSK | 600 | 600 | 600 | 35 | 8.1 | $<$ 1e-4 |
| | QPSK | | | 1,200 | 31 | 10 | |
| | 16QAM | | | 2,400 | 23 | 15.7 | |
| | 64QAM | | | 4,800 | 17 | 17.8 | |

Mbps while using the lab-made transducers with QPSK, 16-QAM and 64-QAM, respectively. The results indicate URadio enables high speed ultrasonic data exchange; URadio can also have a long transmission distance of 10.3 m when using SensComp transducers with BPSK modulation, enabling long range data exchange. It is noteworthy that lab-made transducers' transmission range (27 cm and 35 cm using BPSK for AMF membrane and rGO membrane) is limited by the maximum output power (0.54 watt) of our high bandwidth amplifiers GWBP-AMP-X75 at the transmitter. We also expect the communication range to extend with a better acoustic engineering, which we leave for future work. AMF membrane based transducer has similar BER performance as its rGO membrane based counterpart because of their similar structure. Fig. 5.2 shows the BER performance of URadio equipped with SensComp transducers and AMF/rGO transducers. The URadio system with AMF/rGO transducers can achieve $10^{-5}$ BER at 10 dB SNR using QPSK, and there is a considerable performance gap between systems using QPSK and 16-QAM schemes.

In the second experiment, we evaluate the image transmission performance to validate the high bandwidth transmission capability of the URadio system using rGO

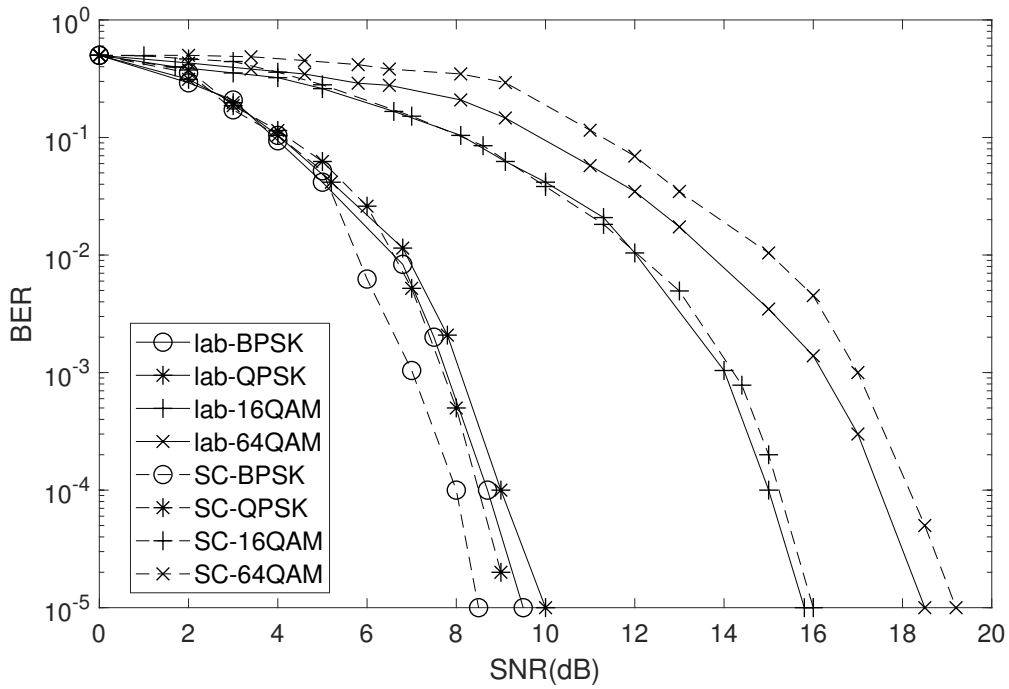


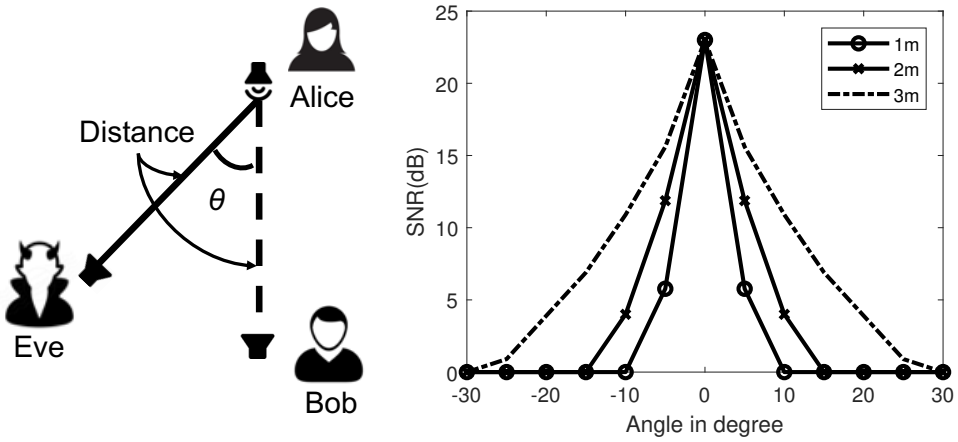

Figure 5.2: BER performance of different transducers using different modulation schemes. SC-BPSK, SC-QPSK, SC-16QAM, SC-64QAM represent the performance of URadio with SensComp transducers at a communication range of 1 m, while lab-BPSK, lab-QPSK, lab-16QAM, lab-64QAM represent the performance of URadio with lab-made AMF and rGO transducers at a communication range of 15 cm.

membrane. We transform a 512 × 512 pixels bmp format Lena image with 8 bit grey scale into bits, and use the URadio system to achieve image transmission at different transmission ranges, such as 15 cm, 20 cm, 25 cm. The entire transmission process takes around 900 ms using 16-QAM at a data rate of 2.4 Mbps, showing that URadio is capable of initiating large data transfer that is very useful for a variety of smart home applications. Fig. 5.3 shows the received Lena pictures across different communication ranges, the quality of which degrades with increasing distances.

(a) (b)

(c) (d)

Figure 5.3: Received Lena pictures using 16-QAM with different distances between Alice and Bob: (a) distance = 15 cm, SNR = 18.8 dB; (b) distance = 20 cm, SNR = 15.4 dB; (c) distance = 25 cm, SNR = 10.86 dB; (d) distance = 30 cm, SNR = 3.9 dB.

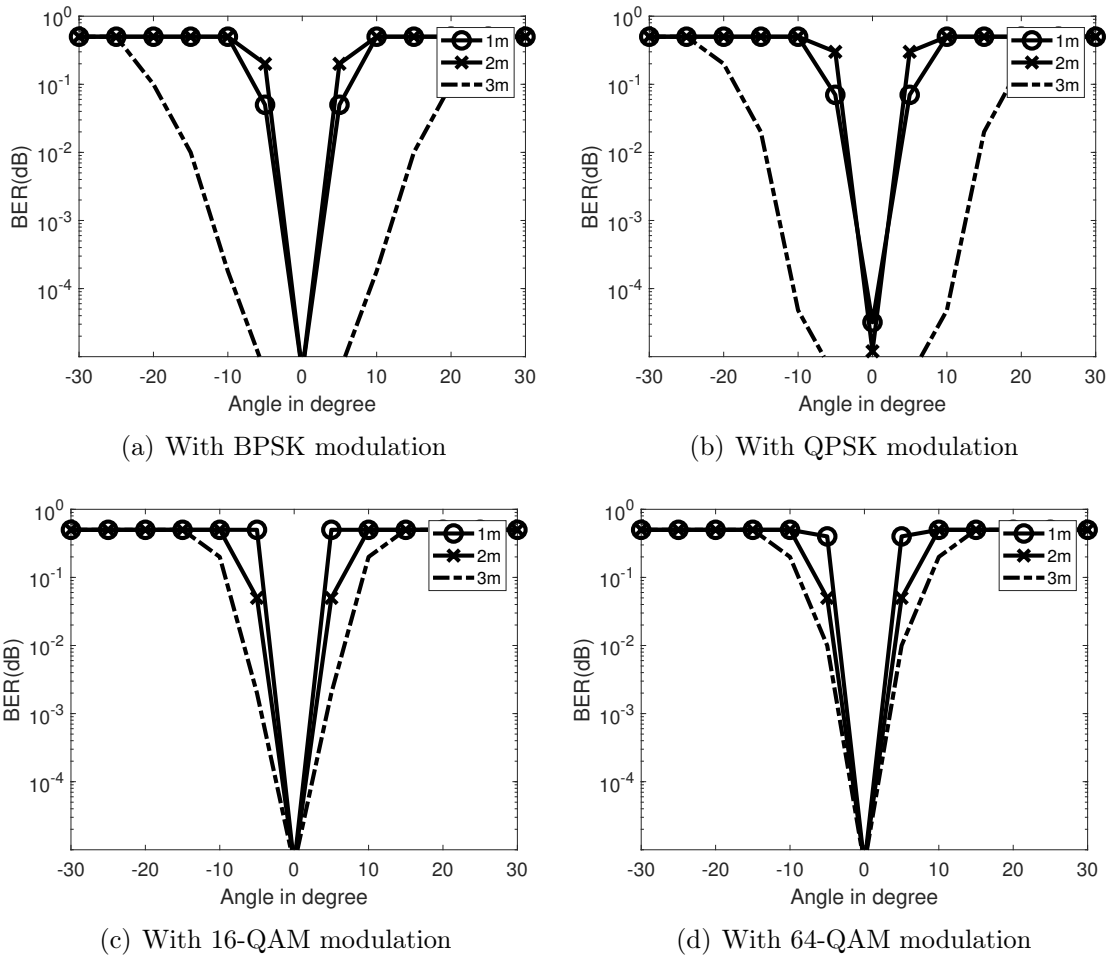



(a) (b)

Figure 5.4: Eavesdropping attacks with an angle $\theta$ between the eavesdropper Eve and the LoS link of the benign transmission between Alice and Bob. The distances between Alice and Bob, Alice and Eve are set as the same: (a) eavesdropping attack experimental setup; (b) SNR of Eve with different eavesdropping angles and distances using BPSK.

## 5.3 Security Evaluation

Ultrasonic signal transmits efficiently over an LoS link, and any angular deviation may result in a significant loss of SNR, which is also the reason why URadio can effectively counter eavesdropping attacks. The URadio system assembled with a pair of SensComp transducers is used to test the relationship between eavesdropping angles, SNR, and BER with different distances between Alice and Eve, as shown in Fig. 5.4 and Fig. 5.5. We can see from Fig. 5.5 that URadio communication can be eavesdropped at a wider angle at 3 m, but a small eavesdropping angle of 5° will still result in an SNR loss of at least 5 dB as shown in Fig. 5.4(b). Moreover, a 10° angular deviation can cause an SNR dip of more than 25 dB, 20 dB, and 10 dB with a distance of 1 m, 2 m, and 3 m, respectively. Notably, higher order modulation schemes are more secure against eavesdroppers, with which the BER performance degrades dramatically when there is a slight angular deviation. This result indicates that eavesdropping URadio's data transfer will suffer from low channel quality, leading to a low




(a) With BPSK modulation

(b) With QPSK modulation

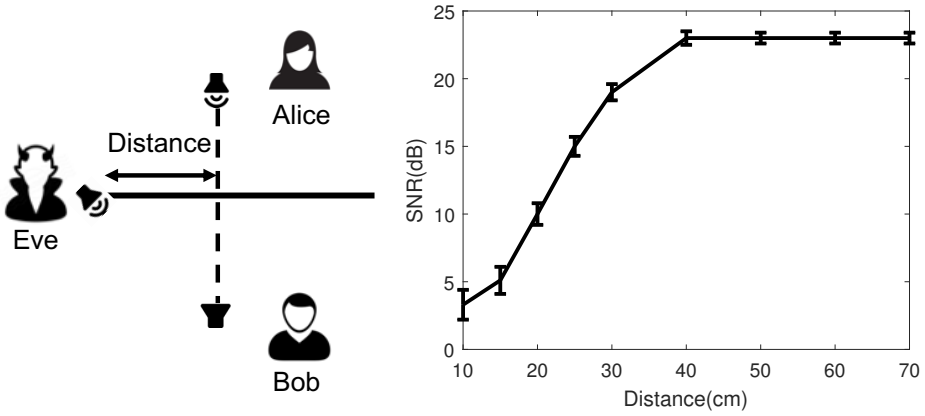
(c) With 16-QAM modulation

(d) With 64-QAM modulation

Figure 5.5: BER performance of an eavesdropper with different eavesdropping angles and different distances.

eavesdropping quality. It is worth-noting that: as the transmission distance increases, the 3dB-SNR-loss transmission angle slightly increases. The results demonstrate the URadio's secure communication capability enabled by ultrasound.

We also evaluate the jamming resilience performance of URadio system (equipped with SensComp transducers) by setting up an experiment as shown in Fig. 5.6. We let Eve continuously transmit an ultrasonic jamming signal to Bob, while Bob is receiving benign signals from Alice. Alice is positioned 5 meters away from Bob; Eve is at different positions on the vertical bisector pointing to Bob. The jamming signal




(a) (b)

Figure 5.6: Eve launches jamming attack to disrupt the communication between Alice and Bob: (a) jamming attack experimental setup (distance between Alice and Bob is 5 m); (b) SNR of Bob for the benign communication under attack.

Table 5.2: Performance comparison.

| Related Systems | Modulation Type | Data Rate (bps) | Range (cm) |
|---|---|---|---|
| U-Wear [5] | 16QAM-OFDM | 2.76K | N/A |
| BackDoor [6] | AM | 4K | 100 |
| Chirp [7] | chirp | 4K | 100 |
| Multi-Tone [8] | MFSK | 800 | N/A |
| Short-Range [10] | QPSK | 200K | 1,200 |
| Indoor [11] | 16QAM-OFDM | 800K | 70 |
| **URadio-SC** | **BPSK-OFDM** | **20K** | **1,030** |
| **URadio-rGO** | **64QAM-OFDM** | **4.8M** | **17** |

URadio-SC is the URadio system with SensComp transducers.
URadio-rGO is the URadio system with rGO transducers.

is a band-limited Gaussian white noise with its power equal to the source power sent by Alice and its bandwidth covering the entire frequency range of SensComp (i.e., 45 kHz - 65 kHz). The result is shown in Fig. 5.6, which indicates that jamming attack can only effectively reduce the SNR of received signal by at least 3 dB when the distance is less than 30 cm, demonstrating URadio's jamming resilience.

## 5.4 Performance Comparison

Table 5.2 compares URadio with other state-of-the-art airborne ultrasonic communication systems according to their maximum transmission range and maximum data rate. As is shown in Table 5.2, when using SensComp transducers for data communication, URadio achieves a longer transmission range. While using rGO transducers, URadio significantly improves the data rate at a short range. URadio so far has the highest data rate (i.e., 4.8 Mbps), which is 6× faster than the previous best system. Therefore, if the data throughput is considered as the first priority, our lab-made transducers with broader bandwidth should be used. On the other hand, if the transmission range is considered as the top priority, Senscomp 600 series could be employed. Compared with previous work that primarily considers a small amount of data exchange, URadio can handle large size file transfer. The high-speed communication capability integrated with security features make URadio well suited to be adopted in secure smart home applications.

# Chapter 6

# Conclusion

In this thesis, we presented URadio, a secure and high data rate ultrasonic communication system. Using a pair of COTS transducers, URadio can achieve an attainable range of 10.3 meter at a data rate of 20 Kbps. We designed two types of new transducers using membranes made of thin materials including Aluminized Mylar Film and reduced Graphene Oxide. The proposed system was able to achieve a record-high data rate of 4.8 Mbps with an attainable range of 17 cm. The relatively short range of lab-made transducers was caused by the limited power upper bound of the power amplifier that could be improved if a higher gain power amplifier is used, as well as the lack of acoustic engineering. Image transmission quality was evaluated to prove that our system can achieve high-speed data exchange in an error-free manner. We evaluated URadio's security performance by measuring eavesdropping angles and jamming attack distances, which corroborates the security of URadio communication.

## Bibliography

[1] Q. Yan, H. Zeng, T. Jiang, M. Li, W. Lou, and Y. T. Hou, "Mimo-based jamming resilient communication in wireless networks," in *Proc. of INFOCOM*, 2014, pp. 2697–2706.

[2] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive mimo: An overview on passive eavesdropping and active attacks," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 21–27, 2015.

[3] C. Pöpper, N. O. Tippenhauer, B. Danev, and S. Capkun, "Investigation of signal and message manipulations on the wireless channel," in *European Symposium on Research in Computer Security*, 2011.

[4] D. Schindel and D. Hutchins, "Applications of micromachined capacitance transducers in air-coupled ultrasonics and nondestructive evaluation," *IEEE transactions on ultrasonics, ferroelectrics, and frequency control*, vol. 42, no. 1, pp. 51–58, 1995.

[5] G. E. Santagati and T. Melodia, "U-wear: Software-defined ultrasonic networking for wearable devices," in *Proc. of MobiSys*, 2015, pp. 241–256.

[6] N. Roy, H. Hassanieh, and R. Roy Choudhury, "Backdoor: Making microphones hear inaudible sounds," in *Proc. of MobiSys*, 2017, pp. 2–14.

[7] H. Lee, T. H. Kim, J. W. Choi, and S. Choi, "Chirp signal-based aerial acoustic communication for smart devices," in *Proc. of INFOCOM*, 2015.

[8] T. Hosman, M. Yeary, J. K. Antonio, and B. Hobbs, "Multi-tone fsk for ultrasonic communication," in *IEEE Instrumentation and Measurement Technology Conference (I2MTC)*, 2010, pp. 1424–1429.

[9] "Silverpush," http://www.silverpush.co/, Accessed on Jan. 29, 2019.

[10] C. Li, D. A. Hutchins, and R. J. Green, "Short-range ultrasonic communications in air using quadrature modulation," *IEEE transactions on ultrasonics, ferroelectrics, and frequency control*, vol. 56, no. 10, 2009.

[11] W. Jiang and W. M. Wright, "Indoor airborne ultrasonic wireless communication using ofdm methods," *IEEE transactions on ultrasonics, ferroelectrics, and frequency control*, vol. 64, no. 9, pp. 1345–1353, 2017.

[12] Q. Zhou, J. Zheng, S. Onishi, M. Crommie, and A. K. Zettl, "Graphene electrostatic microphone and ultrasonic radio," *Proceedings of the National Academy of Sciences*, vol. 112, no. 29, pp. 8942–8946, 2015.

[13] G. Eda, G. Fanchini, and M. Chhowalla, "Large-area ultrathin films of reduced graphene oxide as a transparent and flexible electronic material," *Nature nanotechnology*, vol. 3, no. 5, p. 270, 2008.

[14] W. Jiang and W. M. Wright, "Full-duplex airborne ultrasonic data communication using a pilot-aided qam-ofdm modulation scheme," *IEEE transactions on ultrasonics, ferroelectrics, and frequency control*, vol. 63, no. 8, pp. 1177–1185, 2016.

[15] M. Zhou, Q. Wang, K. Ren, D. Koutsonikolas, L. Su, and Y. Chen, "Dolphin: Real-time hidden acoustic signal capture with smartphones," *IEEE Transactions on Mobile Computing*, 2018.

[16] L. Song and P. Mittal, "Inaudible voice commands," *arXiv preprint arXiv:1708.07238*, 2017.

[17] G. Zhang, C. Yan, X. Ji, T. Zhang, T. Zhang, and W. Xu, "Dolphinattack: Inaudible voice commands," in *Proc. of CCS*, 2017, pp. 103–117.

[18] C. Bolton, S. Rampazzi, C. Li, A. Kwong, W. Xu, and K. Fu, "Blue note: How intentional acoustic interference damages availability and integrity in hard disk drives and operating systems," in *Proc. of IEEE S&P*, 2018.

[19] M. Backes, M. Dürmuth, S. Gerling, M. Pinkal, and C. Sporleder, "Acoustic side-channel attacks on printers." in *Proc. of USENIX Security*, 2010.

[20] T. Trippel, O. Weisse, W. Xu, P. Honeyman, and K. Fu, "Walnut: Waging doubt on the integrity of mems accelerometers with acoustic injection attacks," in *Proc. of EuroS&P*, 2017, pp. 3–18.

[21] Y. Tu, Z. Lin, I. Lee, and X. Hei, "Injected and delivered: Fabricating implicit control over actuation systems by spoofing inertial sensors," in *Proc. of USENIX Security*, 2018.

[22] T. F. Embleton, "Tutorial on sound propagation outdoors," *The Journal of the Acoustical Society of America*, vol. 100, no. 1, pp. 31–48, 1996.

[23] K. Attenborough, "Review of ground effects on outdoor sound propagation from continuous broadband sources," *Applied acoustics*, vol. 24, no. 4, pp. 289–319, 1988.

[24] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1933–1954, 2014.

[25] Senscomp. [Online]. Available: http://www.senscomp.com/pdfs/series-600-instr-grade-ultrasonic-sensor-spec.pdf

[26] M. Eslamian and F. Zabihi, "Ultrasonic substrate vibration-assisted drop casting (svadc) for the fabrication of photovoltaic solar cell arrays and thin-film devices," *Nanoscale research letters*, vol. 10, no. 1, p. 462, 2015.

[27] M. Soumekh, *Synthetic aperture radar signal processing.* New York: Wiley, 1999, vol. 7.